

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): MASUOKA, et al.
Serial No.: Not yet assigned
Filed: July 30, 2003
Title: NETWORK MONITORING METHOD FOR INFORMATION
SYSTEM, OPERATIONAL RISK EVALUATION METHOD,
SERVICE BUSINESS PERFORMING METHOD, AND
INSURANCE BUSINESS MANAGING METHOD
Group: Not yet assigned

LETTER CLAIMING RIGHT OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

July 30, 2003

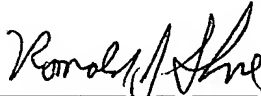
Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s)
hereby claim(s) the right of priority based on Japanese Patent Application No.(s)
2003-048456, filed February 26, 2003.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP


~~James N. Dresser~~ *Ronald J. Shore*
~~Registration No. 22,973~~ *Reg. No. 28,577*

JND/alb
Attachment
(703) 312-6600

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2003年 2月26日

出 願 番 号
Application Number:

特願2003-048456

[ST.10/C]:

[JP2003-048456]

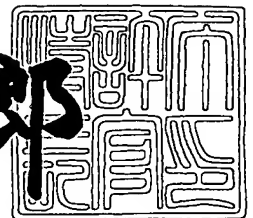
出 願 人
Applicant(s):

株式会社日立製作所

2003年 5月23日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3037876

【書類名】 特許願

【整理番号】 H02013741

【提出日】 平成15年 2月26日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60
G06F 19/00

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所 中央研究所内

 【氏名】 増岡 義政

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所 中央研究所内

 【氏名】 直野 健

【発明者】

 【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所 中央研究所内

 【氏名】 亀山 伸

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100080001

 【弁理士】

 【氏名又は名称】 筒井 大和

 【電話番号】 03-3366-0787

【手数料の表示】

 【予納台帳番号】 006909

 【納付金額】 21,000円

【提出物件の目録】

【物件名】	明細書	1
【物件名】	図面	1
【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 情報システムのネットワーク監視方法及びオペレーショナルリ
スク計量方法

【特許請求の範囲】

【請求項 1】 ネットワークに接続されアプリケーションを実行する 1 つ以上
の第 1 の計算機において、1 つ以上のエージェントを実行して前記第 1 の計算
機内の操作履歴を収集するステップと、

前記ネットワークに接続され前記ネットワークを監視する 1 つ以上の第 2 の計
算機において、前記エージェントが実行されていない前記第 1 の計算機の存在を
監視して記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第 1 の計算機のすべてにおい
て前記エージェントが実行されているか否かを確認するステップとを有すること
を特徴とする情報システムのネットワーク監視方法。

【請求項 2】 ネットワークに接続されアプリケーションを実行する 1 つ以上
の第 1 の計算機において、1 つ以上のエージェントを実行して前記第 1 の計算
機内の操作履歴を収集するステップと、

前記ネットワークに接続され前記ネットワークを監視する 1 つ以上の第 2 の計
算機において、前記ネットワークを流れるパケットを傍受するステップと、

前記第 2 の計算機において、前記傍受したパケットから送信元及び／又は送信
先のアドレスを取り出すステップと、

前記第 2 の計算機において、前記アドレスに対応する前記第 1 の計算機の前記
エージェントに対してメッセージを送信するステップと、

前記第 2 の計算機において、前記送信メッセージに対する応答を確認し、応答
がない前記第 1 の計算機の前記アドレスを記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第 1 の計算機のすべてにおい
て前記エージェントが実行されているか否かを確認するステップとを有すること
を特徴とする情報システムのネットワーク監視方法。

【請求項 3】 ネットワークに接続されアプリケーションを実行する 1 つ以上
の第 1 の計算機において、1 つ以上のエージェントを実行して前記第 1 の計算

機内の操作履歴を収集するステップと、

前記ネットワークに接続され前記ネットワークを監視する 1 つ以上の第 2 の計算機において、前記ネットワークを構成するネットワーク機器と通信して、前記ネットワーク機器に接続された前記第 1 の計算機のアドレスリストを取得するステップと、

前記第 2 の計算機において、前記取得したアドレスリスト内のアドレスに対応する前記第 1 の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第 2 の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第 1 の計算機の前記アドレスを記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第 1 の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのネットワーク監視方法。

【請求項 4】 ネットワークに接続されアプリケーションを実行する 1 つ以上の第 1 の計算機において、1 つ以上のエージェントを実行して前記第 1 の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され前記ネットワークを監視する 1 つ以上の第 2 の計算機において、前記エージェントが実行されていない前記第 1 の計算機の存在を監視して記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第 1 の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのオペレーショナルリスク計量方法。

【請求項 5】 ネットワークに接続されアプリケーションを実行する 1 つ以上の第 1 の計算機において、1 つ以上のエージェントを実行して前記第 1 の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され前記ネットワークを監視する 1 つ以上の第 2 の計算機において、前記ネットワークを流れるパケットを傍受するステップと、

前記第 2 の計算機において、前記傍受したパケットから送信元及び／又は送信先のアドレスを取り出すステップと、

前記第 2 の計算機において、前記アドレスに対応する前記第 1 の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第 2 の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第 1 の計算機の前記アドレスを記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第 1 の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのオペレーショナルリスク計量方法。

【請求項 6】 ネットワークに接続されアプリケーションを実行する 1 つ以上の第 1 の計算機において、1 つ以上のエージェントを実行して前記第 1 の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され前記ネットワークを監視する 1 つ以上の第 2 の計算機において、前記ネットワークを構成するネットワーク機器と通信して、前記ネットワーク機器に接続された前記第 1 の計算機のアドレスリストを取得するステップと、

前記第 2 の計算機において、前記取得したアドレスリスト内のアドレスに対応する前記第 1 の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第 2 の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第 1 の計算機の前記アドレスを記録に残すステップと、

前記記録を検査し、情報システムを構成する前記第 1 の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする情報システムのオペレーショナルリスク計量方法。

【請求項 7】 ネットワークに接続されアプリケーションを実行する顧客企

業所有の1つ以上の第1の計算機において、1つ以上のエージェントを実行して前記第1の計算機内の操作履歴を収集するステップと、

前記ネットワークに接続されサービス事業者の管理の下に設置された1つ以上の第2の計算機において、前記エージェントが実行されていない前記第1の計算機の存在を監視して記録に残すステップと、

前記サービス事業者において、前記記録を検査し、情報システムを構成する前記第1の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする顧客企業のオペレーショナルリスクの正確性を公証するサービス事業の実施方法。

【請求項8】 ネットワークに接続されアプリケーションを実行する顧客企業所有の1つ以上の第1の計算機において、1つ以上のエージェントを実行して前記第1の計算機内の操作履歴を収集するステップと、

前記ネットワークに接続されサービス事業者の管理の下に設置された1つ以上の第2の計算機において、前記ネットワークを流れるパケットを傍受するステップと、

前記第2の計算機において、前記傍受したパケットから送信元及び／又は送信先のアドレスを取り出すステップと、

前記第2の計算機において、前記アドレスに対応する前記第1の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第2の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第1の計算機の前記アドレスを記録に残すステップと、

前記サービス事業者において、前記記録を検査し、情報システムを構成する前記第1の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップとを有することを特徴とする顧客企業のオペレーショナルリスクの正確性を公証するサービス事業の実施方法。

【請求項9】 ネットワークに接続されアプリケーションを実行する顧客企業所有の1つ以上の第1の計算機において、1つ以上のエージェントを実行して前記第1の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され保険業者の管理の下に設置された 1 つ以上の第 2 の計算機において、前記エージェントが実行されていない前記第 1 の計算機の存在を監視して記録に残すステップと、

前記保険業者において、前記記録を検査し、情報システムを構成する前記第 1 の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップと、

を有することを特徴とする顧客企業のオペレーショナルリスクに該当する事象により発生した損失を補填する保険業の運営方法。

【請求項 10】 ネットワークに接続されアプリケーションを実行する顧客企業所有の 1 つ以上の第 1 の計算機において、 1 つ以上のエージェントを実行して前記第 1 の計算機内の操作履歴を収集するステップと、

前記収集した操作履歴から損失の発生した事象を抽出するステップと、

前記抽出した事象における損失額を決定するステップと、

前記ネットワークに接続され保険業者の管理の下に設置された 1 つ以上の第 2 の計算機において、前記ネットワークを流れるパケットを傍受するステップと、

前記第 2 の計算機において、前記傍受したパケットから送信元及び／又は送信先のアドレスを取り出すステップと、

前記第 2 の計算機において、前記アドレスに対応する前記第 1 の計算機の前記エージェントに対してメッセージを送信するステップと、

前記第 2 の計算機において、前記送信メッセージに対する応答を確認し、応答がない前記第 1 の計算機の前記アドレスを記録に残すステップと、

前記保険業者において、前記記録を検査し、情報システムを構成する前記第 1 の計算機のすべてにおいて前記エージェントが実行されているか否かを確認するステップと、

を有することを特徴とする顧客企業のオペレーショナルリスクに該当する事象により発生した損失を補填する保険業の運営方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワーク監視方法及びオペレーショナルリスク計量方法などに関し、特にネットワークを利用した複数の計算機を含む情報処理システムのオペレーショナルリスク計量技術に適用して有効な技術に関する。

【0002】

【従来の技術】

近年、非特許文献1に記載されているように、企業（非営利団体や一般の組織も含む。以下、これらの総称として「企業」という）は、その健全性を維持するためのリスク管理の一方法として、その内部の情報システムの操作ミスや情報システム内で発生した障害などによって受ける損失額をリスクとして計量しようとしている。この種のリスクは、「オペレーショナルリスク（Operational Risk）」と呼ばれており、特に金融機関ではその重要性が高い。どのような事象をオペレーショナルリスクとして判断するか、オペレーショナルリスクに該当する各事象をどのように分類するか、については、前記非特許文献1に、現状の定義が記載されている。

【0003】

また、非特許文献2によれば、オペレーショナルリスクは、例えば、次の方法によって計量できる。まず、過去の企業内部及び外部のデータを収集・蓄積し、損失の発生した事象を示す元となるデータ（以下、「損失イベント（operational loss event）」という）を集める。次に、収集した損失イベントに対し、一定の計算を行うことにより、オペレーショナルリスクを計量する。

【0004】

現在の企業では、ほとんどすべての業務が何らかの形で情報システムを利用して遂行されている。この情報システムは、通常、ネットワークに接続された複数の計算機（端末やサーバなど）で業務アプリケーションを実行させている。そのため、前記損失イベントの収集においては、情報システムの運用管理機能において、エラーログなどの操作履歴情報を取得することが重要である。運用管理機能については、特許文献1や特許文献2などに記載されている。これらの運用管理

機能では、ネットワーク内を流れる情報を傍受することにより、ネットワークに接続された計算機等の構成図を作成することができる。

【0005】

【特許文献1】

米国特許第5948055号明細書

【0006】

【特許文献2】

米国特許第5787252号明細書

【0007】

【非特許文献1】

バーゼル・コミッティ・オン・バンキング・スーパービジョン (Basel Committee on Banking Supervision) 編, 「ワーキング・ペーパー・オン・ザ・レギュラトリ・トリートメント・オブ・オペレーショナル・リスク (Working Paper on the Regulatory Treatment of Operational Risk)」, 国際決済銀行, 2001年9月

【0008】

【非特許文献2】

三菱信託銀行オペレーショナル・リスク研究会編, 「オペレーショナル・リスクのすべて」, 東洋経済新報社, 2002年3月, p. 107-157

【0009】

【発明が解決しようとする課題】

ところで、前記のようなオペレーショナルリスク計量の技術について、本発明者が検討した結果、以下のようなことが明らかとなった。

【0010】

オペレーショナルリスクを計量するためには、企業内部の損失イベントの収集が不可欠である。しかしながら、前記の従来技術では、オペレーショナルリス

クをリスク管理に活用するには、次の点で問題がある。

【 0 0 1 1 】

すなわち、その企業内で業務に用いられているすべての計算機から、損失イベントを収集したか否か、確認する方法がない。そのため、オペレーショナルリスクを計量する際に収集した損失イベントが、その企業内で発生した損失イベントのすべてか否か、又は、オペレーショナルリスク計量のために許容される誤算の範囲で十分か否かが確認できない。

【 0 0 1 2 】

例えば、ある計算機の操作ミスによって、その企業に損失が発生したとする。もし、この計算機が損失イベントの情報収集の対象になっていないとき、計量されたオペレーショナルリスクは、不当に低く算出されてしまうことになる。これでは、企業の経営の一環としてオペレーショナルリスクの管理を適切に行うことも、オペレーショナルリスクの管理を適切に行っていることを外部に示すこともできない。

【 0 0 1 3 】

そこで、本発明の第 1 の目的は、オペレーショナルリスク計量のために、企業内で業務に用いられているすべての計算機から損失イベントを収集したか否かを確認することができるネットワーク監視方法を提供することである。

【 0 0 1 4 】

本発明の第 2 の目的は、前記ネットワーク監視方法を用いた、オペレーショナルリスク計量方法を提供することである。

【 0 0 1 5 】

本発明の第 3 の目的は、前記ネットワーク監視方法を用いた、オペレーショナルリスク計量のためのサービス方法を提供することである。

【 0 0 1 6 】

本発明の前記並びにその他の目的と新規な特徴は、本明細書の記述及び添付図面から明らかになるであろう。

【 0 0 1 7 】

【課題を解決するための手段】

本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、次のとおりである。

【 0 0 1 8 】

すなわち、本発明によるネットワーク監視方法及びオペレーショナルリスク計量方法においては、企業のネットワークに接続されアプリケーションを実行する1つ以上の第1の計算機（業務実行計算機）に、その計算機内で発生した損失イベントを収集するためのエージェントを1つ以上設ける。また、その企業のネットワークに接続されネットワークを監視する第2の計算機（ネットワーク監視サーバ機）を1つ以上設ける。当該第2の計算機は、当該ネットワークを監視し、第1の計算機の中に、前記エージェントが設けられていない計算機があれば、その旨を記録に追加する。

【 0 0 1 9 】

前記第2の計算機が前記ネットワークを監視する方法としては、当該ネットワークを流れるパケットを傍受し、当該パケットから送信元及び／又は送信先のアドレスを取り出し、取り出したアドレスに対応する計算機の前記エージェントに対してメッセージを送信し、当該送信メッセージに対する応答を確認する方法がある。

【 0 0 2 0 】

また、前記第2の計算機が前記ネットワークを監視する他の方法としては、前記ネットワークがネットワーク機器（ルータなど）に接続されていて、当該ネットワーク機器がパケットを中継した計算機のアドレスリストを保持している場合は、前記第2の計算機が前記ネットワーク機器と通信して当該アドレスリストを取得し、当該アドレスリスト内のアドレスに対応する計算機の前記エージェントに対してメッセージを送信し、当該送信メッセージに対する応答を確認する方法もある。この場合は、パケットを傍受する必要がないため、工数を軽減することができる。

【 0 0 2 1 】

また、オペレーショナルリスク計量方法としては、前記第1の計算機内で発生した損失イベントを収集するためのエージェントを実行し、前記第1の計算機内

の操作履歴を収集し、当該操作履歴から損失の発生した事象を抽出し、当該事象における損失額を決定し、オペレーショナルリスクを計量する方法がある。

【 0 0 2 2 】

したがって、前記ネットワーク監視方法及び前記オペレーショナルリスク計量方法によれば、前記エージェントによって収集された損失イベントから、オペレーショナルリスクを計量することができるだけでなく、前記第 2 の計算機の前記記録を検査することにより、企業内で業務に用いられる計算機すべてにおいて損失イベントを収集したことを確認することができる。

【 0 0 2 3 】

すなわち、もし、前記記録に何も記載がなければ、企業内で業務に用いられるすべての計算機に前記エージェントが設けられており、すべての計算機から損失イベントが収集されたことを確認することができる。あるいはもし、前記記録に記載があれば、当該記録に記載された、前記エージェントが設けられていない計算機については、別途、手作業や聞き取りによる調査を行うことにより、企業内のすべての前記計算機から損失イベントを収集することができる。

【 0 0 2 4 】

また、情報システムを保有する企業に対して、別のサービス事業者が、前記第 2 の計算機を設置し、前記企業の情報システムのネットワークに接続することにより、当該企業のオペレーショナルリスクの正確性を公証するサービスを提供することができる。

【 0 0 2 5 】

また、保険業者等が前記オペレーショナルリスク計量方法を顧客企業の情報システムに適用することにより、前記顧客企業のオペレーショナルリスクに該当する事象により発生した損失を正確に計量することが可能となり、当該損失を補填したり、当該計量結果に基づいて保険料を決定したりする保険業を運営することができる。

【 0 0 2 6 】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。なお、実施の形

態を説明するための全図において、同一部材には同一の符号を付し、その繰り返しの説明は省略する。

【 0 0 2 7 】

(ハードウェア構成)

図 1 は、本発明の一実施の形態における情報システムのハードウェア構成を示す図である。本実施の形態における企業の情報システム 1 0 0 は、ネットワーク 1 0 1 を有している。ネットワーク 1 0 1 は、企業内の各計算機を、リンク 1 0 2 によって接続している。リンク 1 0 2 は、有線でも無線でもよい。また、図 1 に図示していないが、ネットワーク 1 0 1 は、企業外の計算機と通信するためのリンクを有していてもよい。

【 0 0 2 8 】

情報システム 1 0 0 は、3 種類の計算機を有している。具体的には、業務実行計算機（第 1 の計算機）1 0 3 a, 1 0 3 b, …、運用管理サーバ機 1 0 4、ネットワーク監視サーバ機（第 2 の計算機）1 0 5 である。

【 0 0 2 9 】

業務実行計算機 1 0 3 a, 1 0 3 b, …は、具体的には端末、パーソナルコンピュータ、サーバ計算機、メインフレーム、ネットワーク機器などであり、ネットワーク 1 0 1 に接続され、業務実行計算機 1 0 3 a, 1 0 3 b, …の間で必要に応じて通信しながら、情報システム 1 0 0 を有する企業の業務を分担して実行する。図 1 に図示していないが、業務実行計算機 1 0 3 a, 1 0 3 b, …は、1 つ以上のプロセッサ、記憶装置、ネットワークインタフェースを有している。また、業務実行計算機 1 0 3 a, 1 0 3 b, …のそれぞれは、その利用方法によって、磁気ディスクや外部記憶装置を備えている場合がある。磁気ディスクや外部記憶装置も、図 1 には図示していない。

【 0 0 3 0 】

運用管理サーバ機 1 0 4 は、図 1 では 1 つしか図示していないが、複数設けられていてもよい。運用管理サーバ機 1 0 4 は、ネットワーク 1 0 1 に接続されている。運用管理サーバ機 1 0 4 は、損失イベントを収集し、オペレーショナルリスクを計算するための計算機である。図 1 に図示していないが、1 つ以上のプロ

セッサ、記憶装置、ネットワークインタフェースを有している。

【0031】

ネットワーク監視サーバ機105は、図1では1つしか図示していないが、複数設けられていてもよい。ネットワーク監視サーバ機105は、ネットワーク101に接続されている。ネットワーク監視サーバ機105は、ネットワーク101を監視し、後述するエージェント110が設けられていない計算機が情報システム100に接続されていることを監視、検出するための計算機である。図1に図示していないが、1つ以上のプロセッサ、記憶装置、ネットワークインタフェースを有している。

【0032】

なお、本実施の形態では、業務実行計算機103a、103b、…、運用管理サーバ機104、ネットワーク監視サーバ機105をそれぞれ別の筐体の計算機として扱うが、実際にはどれか2つ、または3種類すべてが、同じ筐体に格納されていてもよい。

【0033】

(ソフトウェア構成)

図1を用いて、本実施の形態のソフトウェア構成、すなわちプログラムとデータの構成を説明する。

【0034】

業務実行計算機103a、103b、…上では、エージェント110が実行される。エージェント110は、データ収集部111と確認応答部112を含むプログラムで、業務実行計算機103a、103b、…のプロセッサにより実行される。

【0035】

データ収集部111は、業務実行計算機103a、103b、…内の履歴情報115a、115b、…の内容を一定間隔で読み込み、ネットワーク101を通して運用管理サーバ機104のデータ集計部131へ送信する。

【0036】

確認応答部112は、ネットワーク監視サーバ機105の検出部122から問

合せメッセージが送られてくるのを待ち、当該問い合わせメッセージが送られてきたら、送信元の検出部 1 2 2 に応答メッセージを送信する。図 4 を用いて後述するが、検出部 1 2 2 は、当該問合せメッセージを用いることにより、業務実行計算機 1 0 3 a, 1 0 3 b, … 上でエージェント 1 1 0 が実行されているか否かを確認する。

【 0 0 3 7 】

図 1 に図示していないが、業務実行計算機 1 0 3 a, 1 0 3 b, … 上では、エージェント 1 1 0 の他に、企業の業務を行うアプリケーションプログラムも 1 つ以上実行される。当該アプリケーションのそれぞれは、過去のログや、エラーメッセージや、実行経過のトレース情報や、稼動統計情報を、履歴情報 1 1 5 a, 1 1 5 b, … に出力している。履歴情報 1 1 5 a, 1 1 5 b, … は、磁気ディスク上のファイルや、運用コマンドの出力結果などの形で、エージェント 1 1 0 のデータ収集部 1 1 1 から、データとして参照可能である。

【 0 0 3 8 】

運用管理サーバ機 1 0 4 では、3 つのプログラムが実行される。すなわち、データ集計部 1 3 1、計量部 1 3 2、及び結果表示部 1 3 3 である。これらのプログラムの動作は、図 3 を用いて後でより詳細に説明するが、データ集計部 1 3 1 は、エージェント 1 1 0 のデータ収集部 1 1 1 から送信されてきた履歴情報を集計し、計量部 1 3 2 はデータ集計部 1 3 1 の集計結果からオペレーショナルリスクを計量し、結果表示部 1 3 3 は計量したオペレーショナルリスクを表示する。なお、その他のプログラムが、運用管理サーバ機 1 0 4 で実行されてもよい。

【 0 0 3 9 】

ネットワーク監視サーバ機 1 0 5 では、パケット監視部 1 2 1 と、検出部 1 2 2 の、2 つのプログラムが実行される。パケット監視部 1 2 1 は、ネットワーク監視サーバ機 1 0 5 が備えるネットワークインタフェースを利用し、ネットワーク 1 0 1 を流れるパケットを傍受する。当該パケットの構造及び内容を図 2 に示す。検出部 1 2 2 は、パケット監視部 1 2 1 が傍受したパケットを受け取り、そのパケットから送信元のアドレスと送信先のアドレスを取り出して、そのアドレスが割り当てられた業務実行計算機 1 0 3 a, 1 0 3 b, … においてエージェン

ト 110 が実行されているか否か確認する。また、検出部 122 は、当該処理のため、2 種類のデータ、すなわちアドレスリスト 125 と監視ログ 126 を保持する。アドレスリスト 125 は、通常主記憶内に格納されるが、磁気ディスク上でもよい。監視ログ 126 は、通常磁気ディスク内に格納される。なお、検出部 122 の動作は、後で図 4 を用いてより詳しく説明する。

【0040】

なお、図 1 には図示していないが、各計算機にはオペレーティング・システムが主記憶にロードされ、当該計算機のプロセッサにより実行される。前記のエージェント 110 などの各プログラムは、当該オペレーティング・システムによって実行を管理されている。また、前記の各プログラムは、必要に応じて、当該オペレーティング・システムに要求を出すことにより、ネットワーク通信、ファイルや磁気ディスク上のデータへのアクセスなどを行うことができる。

【0041】

なお、本実施の形態において、業務実行計算機 103 a, 103 b, …のエージェント 110、データ収集部 111、確認応答部 112、運用管理サーバ機 104 のデータ集計部 131、計量部 132、結果表示部 133、及びネットワーク監視サーバ機 105 のパケット監視部 121、検出部 122 は、いずれもプログラムとして取り扱ったが、これらと同等の機能を有していれば、プログラム以外のものであってもよい。

【0042】

(ネットワーク通信)

図 1 に示すように、ネットワーク 101 は、業務実行計算機 103 a, 103 b, …、運用管理サーバ機 104、及びネットワーク監視サーバ機 105 を相互接続する。

【0043】

ネットワークへの接続について、より具体的に述べると、前記各計算機は、それぞれネットワークインタフェース（図 1 では図示していない）を有し、このネットワークインタフェースがリンク 102 を通してネットワーク 101 に接続されている。

【 0 0 4 4 】

それぞれのネットワークインタフェースには、一意なネットワークアドレス（以下「アドレス」と略す）を割り当てる。このアドレスにより、各計算機間の通信は、次のように実現される。すなわち、送信する側が送信先のアドレスと、送りたいデータを格納している主記憶装置上の領域を指定して、自分のネットワークインタフェースに司令を送ることにより、ネットワーク 1 0 1 を経由して、パケット 2 0 0（図 2）が送信される。パケット 2 0 0 は、前記送信先のアドレスが割り当てられたネットワークインタフェースによって受信され、受信する側で指定した主記憶装置上の領域に書き込まれる。図 2 に示すように、パケット 2 0 0 は、送信先アドレス 2 0 1、送信元アドレス 2 0 2、データ 2 0 3 を含む。

【 0 0 4 5 】

以上の、「各ネットワークインタフェースに一意のアドレスを割り当てたとき、送信側が送信先のアドレスを指定することによって、送信したいデータが、指定したアドレスが割り当てられたネットワークインタフェースを有する装置に正しく届けられる」という機能を実現する通信方式についてのより具体的な説明は、文献「W. Richard Stevens, “UNIX（登録商標） Network Programming”, Prentice-Hall, p. 171-196」に述べられている。本実施の形態の情報システムにおいては、当該通信方式が確立しているものとし、本明細書では、当該通信方式についてのこれ以上の詳細な説明は省略する。

【 0 0 4 6 】

（オペレーショナルリスク計量方法）

図 3 に、本実施の形態におけるオペレーショナルリスクの計量方法を示す。本実施の形態では、オペレーショナルリスクの計量は、図 1 の運用管理サーバ機 1 0 4 のデータ集計部 1 3 1、計量部 1 3 2、及び結果表示部 1 3 3 によって行われる。

【 0 0 4 7 】

まず、データ集計部 1 3 1 は、業務実行計算機 1 0 3 a, 1 0 3 b, …上のエージェント 1 1 0 から送信された履歴情報を受信する（ステップ S 3 0 1）。次

に、データ集計部131は、受信した履歴情報の内容を解析して、損失イベントに該当する事象なのか、どのような種類の損失イベントなのかを、判定結果から損失イベントを抽出する（ステップS302）。より具体的には、前記判定には、例えば履歴情報に含まれるエラーメッセージがあらかじめ登録された文字列パターンと一致するか否かを検査する手法や、履歴情報の内容を適当なディスプレイに表示させて、表示を見た企業の担当者が該当する損失イベントを選択肢から選び、入力するなどの手法を用いる。

【0048】

次に、データ集計部131は、抽出した損失イベントに対し、企業が被った損失の額を決定する（ステップS303）。より具体的には、例えば抽出した損失イベントのそれぞれにおいて、発生日時、発生場所、損失イベントの種類をディスプレイに表示し、ディスプレイを見た担当者が過去の事故報告書を参照して、当該損失イベントと発生日時と発生場所が一致する報告書を抽出し、当該報告書に記載の損失額を当該損失イベントの損失額として入力するなどの手法を用いる。

【0049】

次に、データ集計部131は、ステップS303で作成した、抽出した損失イベントと損失額の組合せを、運用管理サーバ機104の記憶装置に蓄積する（ステップS304）。

【0050】

次に、計量部132は、データ集計部131が記憶装置に蓄積した、損失イベントと損失額の組合せから、オペレーショナルリスクを計算する（ステップS305）。より具体的な計算方法としては、例えば、前記非特許文献2に記載された方法を用いればよい。計量部132は、計算結果を、結果表示部133に渡す。

【0051】

前記計算結果を渡された結果表示部133は、オペレーショナルリスクの計算結果を、ディスプレイ等の出力装置に表示したり、記憶装置中のファイルに格納したり、ネットワーク101を通して他の計算機に送信したりして、企業が当該

計算結果をリスク管理に利用できるようにする（ステップ S 3 0 6）。

【 0 0 5 2 】

（エージェントの設けられていない計算機の検出方法）

図 4 に、本実施の形態において、エージェントの設けられていない計算機が情報システム 1 0 0 のネットワーク 1 0 1 に接続されていないか否か検出する方法を示す。この処理は、ネットワーク監視サーバ機 1 0 5 の検出部 1 2 2 において行われる。

【 0 0 5 3 】

まず、検出部 1 2 2 は、パケット監視部 1 2 1 から渡されたパケット 2 0 0 （図 2）から、送信元アドレスを取り出す（ステップ S 4 0 1）。次に、アドレスリスト 1 2 5 を参照し、取り出した送信元アドレス 2 0 2 が、アドレスリスト 1 2 5 に登録されているか否かを調べる（ステップ S 4 0 2）。もし、当該送信元アドレス 2 0 2 が、アドレスリスト 1 2 5 に登録されていれば、ステップ S 4 0 9 に移行する（ステップ S 4 0 3）。もし、登録されていなければ、送信元アドレス 2 0 2 に該当する計算機上のエージェント 1 1 0 を宛先とする問い合わせメッセージを作成し、ネットワーク 1 0 1 に送信する（ステップ S 4 0 4）。

【 0 0 5 4 】

さらに、検出部 1 2 2 は、送信した問い合わせメッセージに対する応答がネットワーク監視サーバ機 1 0 5 に到来するのを一定時間待つ（ステップ S 4 0 5）。具体的な待ち時間は、企業において、設定できるようにすれば良い。もし、一定時間内に応答が到着したら（ステップ S 4 0 6）、アドレスリスト 1 2 5 に、ステップ S 4 0 1 で取り出した送信元アドレス 2 0 2 を追加する（ステップ S 4 0 8）。もし、応答が到着しなかったら、監視ログ 1 2 6 に、ステップ S 4 0 1 で取り出した送信元アドレス 2 0 2 を追加する（ステップ S 4 0 7）。ステップ S 4 0 7 では、後日の調査のために、監視ログ 1 2 6 に、送信元アドレス 2 0 2 だけではなく、現在の時刻、パケットの内容なども追加してもよい。また、ステップ S 4 0 7 では、担当者が直ちに調査を始められるように、当該担当者の端末にメッセージを表示したりする処理を実行してもよい。検出部 1 2 2 は、ステップ S 4 0 7、ステップ S 4 0 8 のどちらかを実行後、ステップ S 4 0 9 に移行す

る。

【0055】

次に、検出部122は、ステップS401からステップS408までの各ステップを、パケット監視部から渡されたパケット200（図2）の送信先アドレス201についても行う（ステップS409）。

【0056】

以上の手順により、ネットワーク101に、エージェントの設けられていない計算機が接続されていた場合、当該計算機がネットワーク101を通して通信した時点で当該計算機のアドレスを監視ログ126に残すことができる。したがって、オペレーショナルリスクの計量時に、監視ログ126を検査することにより、企業内で業務に用いているすべての計算機から損失イベントを抽出したか否かを確認することができる。

【0057】

すなわち、本実施の形態によれば、ネットワーク監視サーバ機105の監視ログ126に、何も記載がなければ、企業内で業務に用いられる計算機すべてにエージェント110が設けられていることとなり、損失イベントがすべての前記計算機から収集されたことを確認することができる。もし、監視ログ126に記載があれば、監視ログ126に記載された、エージェント110が設けられていない計算機については、別途、手作業や聞き取りによる調査を行うことにより、企業内のすべての計算機から損失イベントを収集することが可能である。

【0058】

（ネットワーク監視方法の変形例）

本実施の形態では、ネットワーク101を流れるパケット200（図2）をネットワーク監視サーバ機105のパケット監視部121が傍受し、検出部122に渡すことによって、エージェントの設けられていない計算機を検出している。以下にその変形例を2つ述べる。

【0059】

第1の変形例は、情報システムのネットワークが、実際はサブネットワークの組合せから構成されている場合に用いられる。図5は、第1の変形例における情

報システムのハードウェア及びソフトウェアを示す構成図である。図5では、企業の情報システム500の各計算機を接続しているのは、2つのサブネットワーク501A、501Bと、2つのサブネットワーク間でパケットを中継するルータ502などのネットワーク機器である。情報システム500では、業務実行計算機503Aa、503Ab、…、503Ba、503Bb、…は、2つのサブネットワーク501A、501Bに分散して接続されている。より具体的には、業務実行計算機503Aa、503Ab、…は、サブネットワーク501Aに、業務実行計算機503Ba、503Bb、…は、サブネットワーク501Bに接続されている。なお、図5には示されていないが、ネットワーク監視サーバ機505A、505Bには、図1に示す構成と同様に、検出部、アドレスリスト及び監視ログなどが含まれる。また、サブネットワーク501A、501Bには、運用管理サーバ機が接続される。

【0060】

この場合、ネットワーク監視サーバ機505A、505Bは、それぞれのサブネットワーク501A、501Bに対し、1つ以上接続する構成にすればよい。図5では、ネットワーク監視サーバ機505Aはサブネットワーク501Aに接続し、パケット監視部121がサブネットワーク501Aのパケットを傍受するようにする。また、ネットワーク監視サーバ機505Bはサブネットワーク501Bに接続し、パケット監視部121がサブネットワーク501Bのパケットを傍受するようにする。

【0061】

これにより、ネットワーク監視サーバ機が一つのサブネットワークだけに接続されている結果、他のサブネットワーク内を流れるパケットを取得できなくなるおそれを防ぐことができる。なお、ここでは、図5を用いて、サブネットワークが2つの場合について説明したが、サブネットワークが3つ以上の場合も同様である。

【0062】

第2の変形例は、情報システム100のネットワーク101が、1つ以上のスイッチ又はルータなどのネットワーク機器に接続されていて、当該ネットワーク

機器が、過去に自分がパケットを中継した計算機のアドレスのリストを保持していて、当該リストを運用コマンド等によって一覧表示する機能を持っている場合である。

【0063】

当該ネットワーク機器がこのような機能を持っている場合は、ネットワーク監視サーバ機105は、パケット監視部121に代えて、一定間隔で当該ネットワーク機器から前記アドレスの一覧表示を取得し、取得したアドレスのリストを検出部122に渡せばよい。

【0064】

これにより、ネットワーク監視サーバ機105は、自分でネットワーク101を流れるパケットを傍受する必要がなくなり、図4に示すステップS401が不要となり、必要な処理能力を軽減することができる。

【0065】

(応用例1)

本実施の形態のネットワーク監視サーバ機105を用いて、下記のようなサービス事業を実施することができる。すなわち、情報システム100を保有する企業に対し、別のサービス事業者が、当該企業が保有するネットワーク監視サーバ機105の代わりに、当該サービス事業者の保有するネットワーク監視サーバ機を、前記企業の情報システム100のネットワーク101に接続する。当該ネットワーク監視サーバ機は、監視ログ126の内容を、当該企業が改変できないように暗号化している他は、これまでに説明したネットワーク監視サーバ機105と同じである。前記サービス事業者は、前記企業から料金を取り、前記ネットワーク監視サーバ機の監視ログ126の内容を、当該企業及び当該サービス事業者とは異なる第三者に公証する。

【0066】

このサービスにより、当該企業は、計量したオペレーショナルリスクが、当該企業内で業務に使うすべての計算機から損失イベントを抽出した結果であると、第三者により説得力のある形で示すことができる。また、当該サービス事業者は、前記の公証サービスを行うことによって、当該企業から収益を上げることがで

きる。

【 0 0 6 7 】

(応用例 2)

本実施の形態の方法を用いて、下記のような保険業を実施することができる。
すなわち、保険業者は、顧客企業から保険料を徴収し、もし当該企業に、オペレーショナルリスクに該当する原因により損失が発生した場合は、その損失に応じた保険金を支払う。ここで、保険業者は、当該顧客企業の情報システムにおいて、当該顧客企業の保有する業務実行計算機 1 0 3 a, 1 0 3 b, …においてエージェント 1 1 0 を実行し、さらに運用管理サーバ機 1 0 4 とネットワーク監視サーバ機 1 0 5 をネットワーク 1 0 1 に接続する。

【 0 0 6 8 】

これにより、当該保険業者は、顧客企業のオペレーショナルリスクを正確に計量できる。そのため、リスクの大きさに応じて保険料を増減するなどのきめ細かな対応が可能となり、オペレーショナルリスクの小さい顧客企業に、より安い保険料を提示することにより保険の魅力を高めたり、リスクの大きい企業から安すぎる保険料しか取っていなかったために、保険金支払いにより損失を被ってしまう危険を低減したりできるようになる。

【 0 0 6 9 】

以上、本発明者によってなされた発明をその実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【 0 0 7 0 】

【発明の効果】

本願において開示される発明のうち、代表的なものによって得られる効果を簡単に説明すれば、以下のとおりである。

【 0 0 7 1 】

(1) 業務実行計算機のエージェントによって収集された損失イベントから、オペレーショナルリスクを計算できるだけでなく、ネットワーク監視サーバ機の記録を検査することにより、企業内で業務に用いられる計算機すべてにおいて損

失イベントを収集したか否かを確認することができる。

【0072】

(2) 顧客企業内で業務に用いられる計算機のすべてから、損失イベントを収集したことを、第三者に対して保証するサービス事業を行い、収益を上げることができる。

【0073】

(3) 保険業者等が前記オペレーショナルリスク計量方法を顧客企業の情報システムに適用することにより、前記顧客企業のオペレーショナルリスクに該当する事象により発生した損失を正確に計量することが可能となり、当該損失を補填したり、当該計量結果に基づいて保険料を決定したりする保険業を運営することができる。

【図面の簡単な説明】

【図1】

本発明の一実施の形態における情報システムのハードウェア及びソフトウェアの構成を示す図である。

【図2】

本発明の一実施の形態における、パケットの構造と内容を示す図である。

【図3】

本発明の一実施の形態における、運用管理サーバ機において実行する、オペレーショナルリスクの計量方法を示す流れ図である。

【図4】

本発明の一実施の形態において、ネットワーク監視サーバ機の検出部の動作を示す流れ図である。

【図5】

本発明の一実施の形態の第1の変形例において、情報システムがルータと1つ以上のサブネットワークから構成されている場合の、ハードウェア及びソフトウェアの構成を示す図である。

【符号の説明】

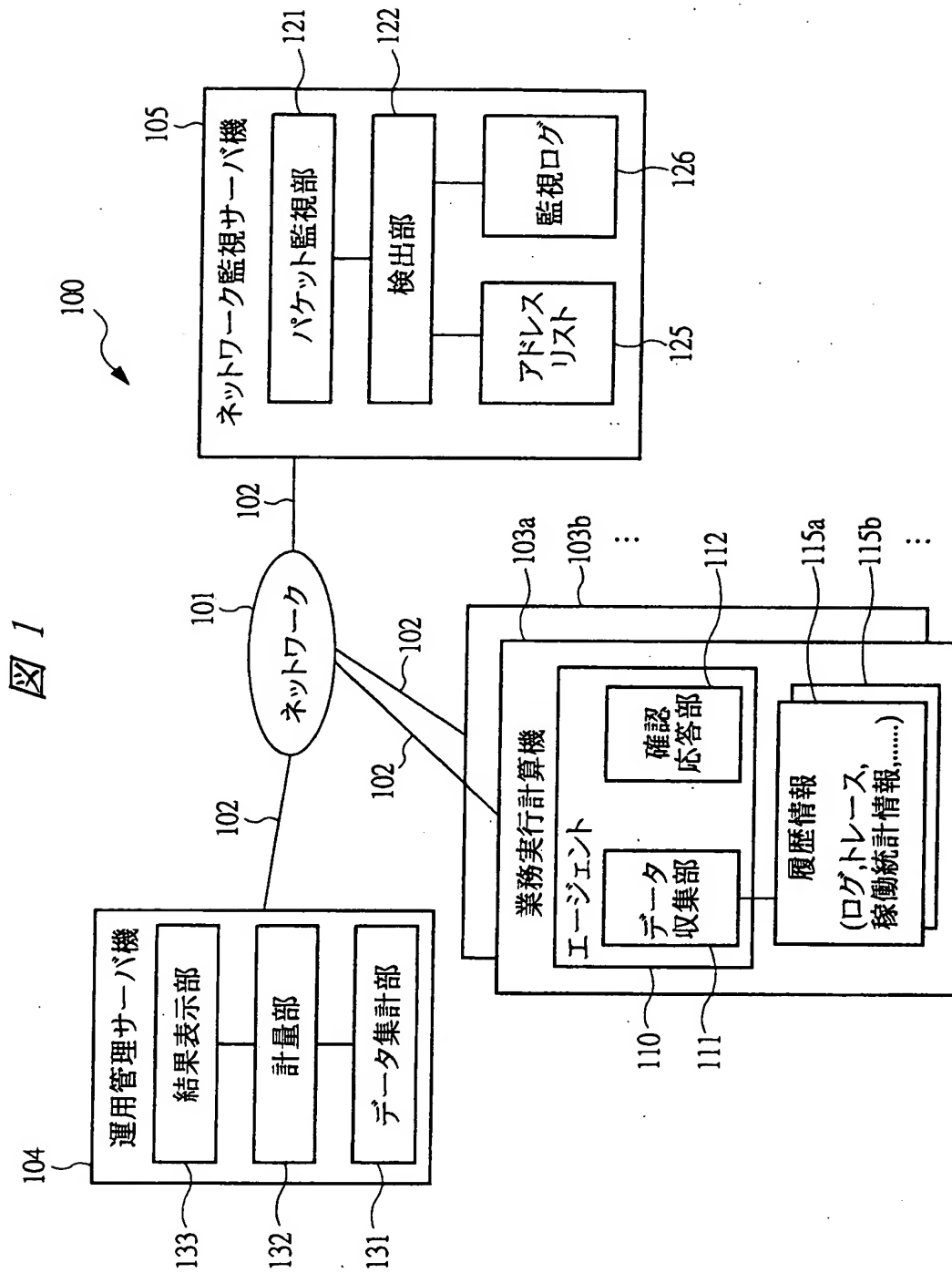
100, 500 情報システム

101 ネットワーク
102 リンク
103a, 103b, 503Aa, 503Ab, 503Ba, 503Bb, ...
業務実行計算機
104 運用管理サーバ機
105, 505A, 505B ネットワーク監視サーバ機
110 エージェント
111 データ収集部
112 確認応答部
115a, 115b, ... 履歴情報
121 パケット監視部
122 検出部
125 アドレスリスト
126 監視ログ
131 データ集計部
132 計量部
133 結果表示部
200 パケット
201 送信先アドレス
202 送信元アドレス
203 データ
501A, 501B サブネットワーク
502 ネットワーク機器 (ルータ)

【書類名】

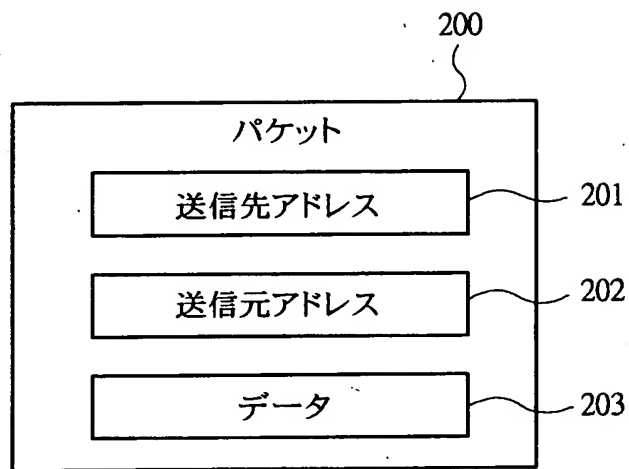
図面

【図 1】



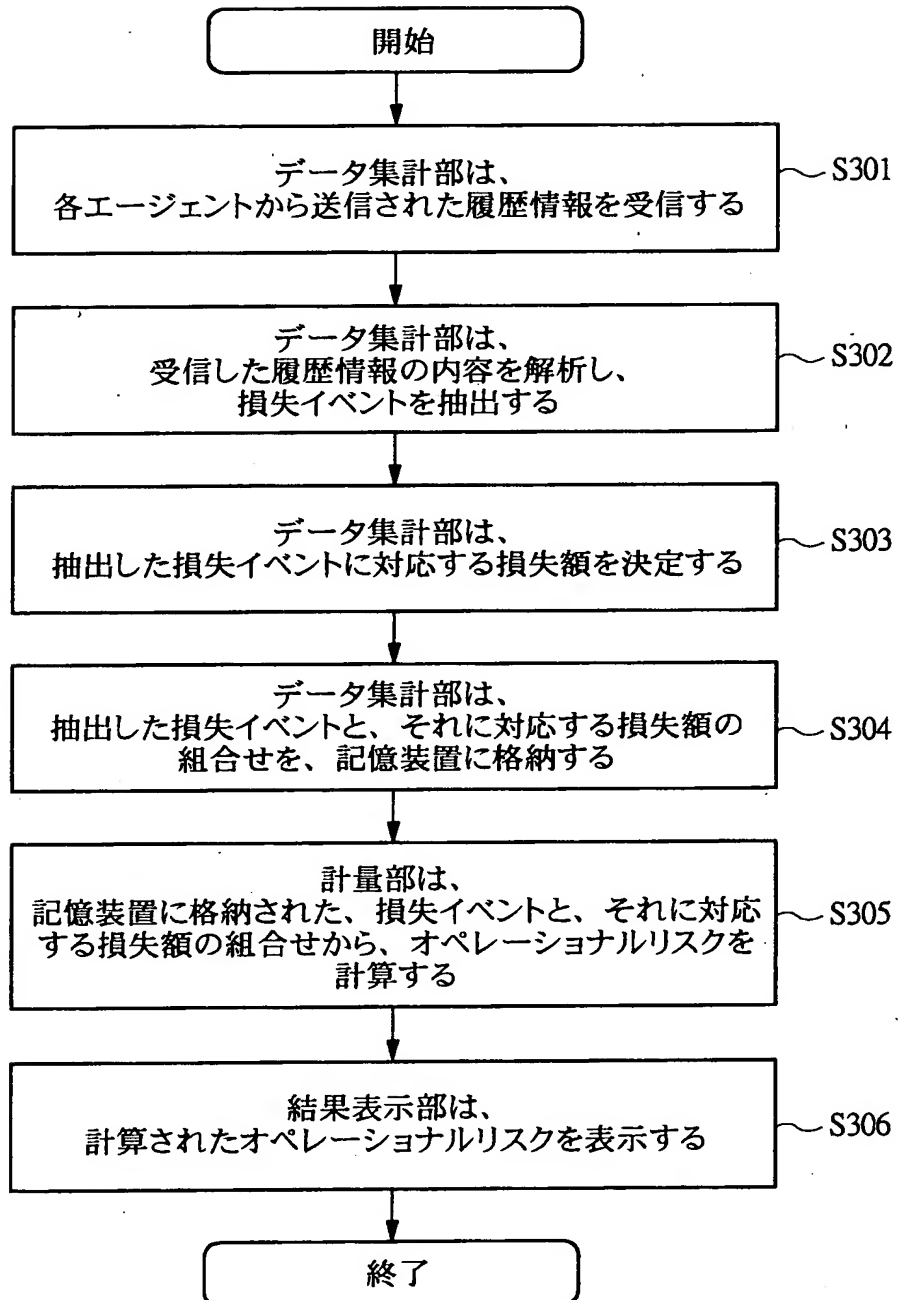
【図 2】

図 2



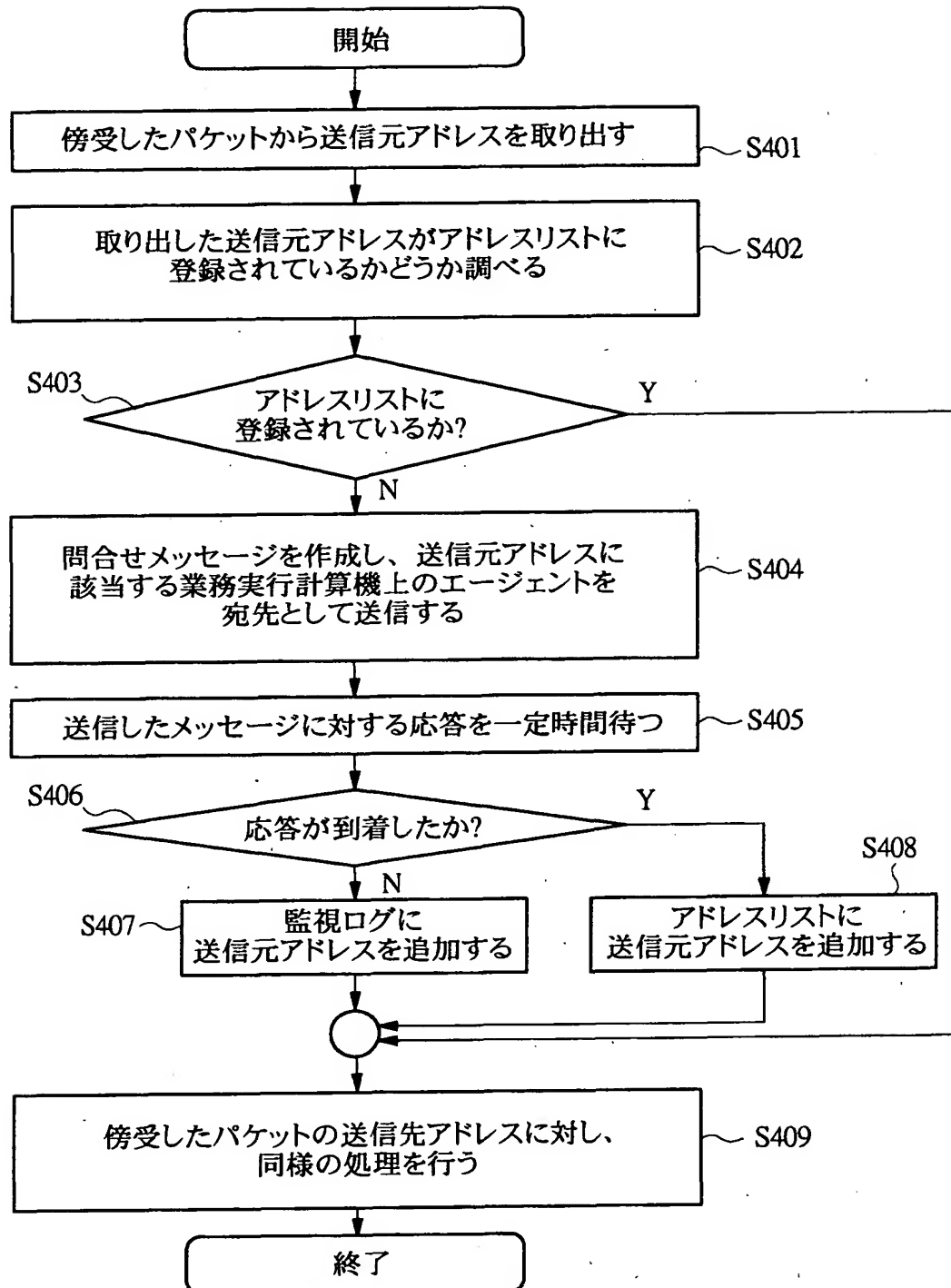
【図 3】

図 3

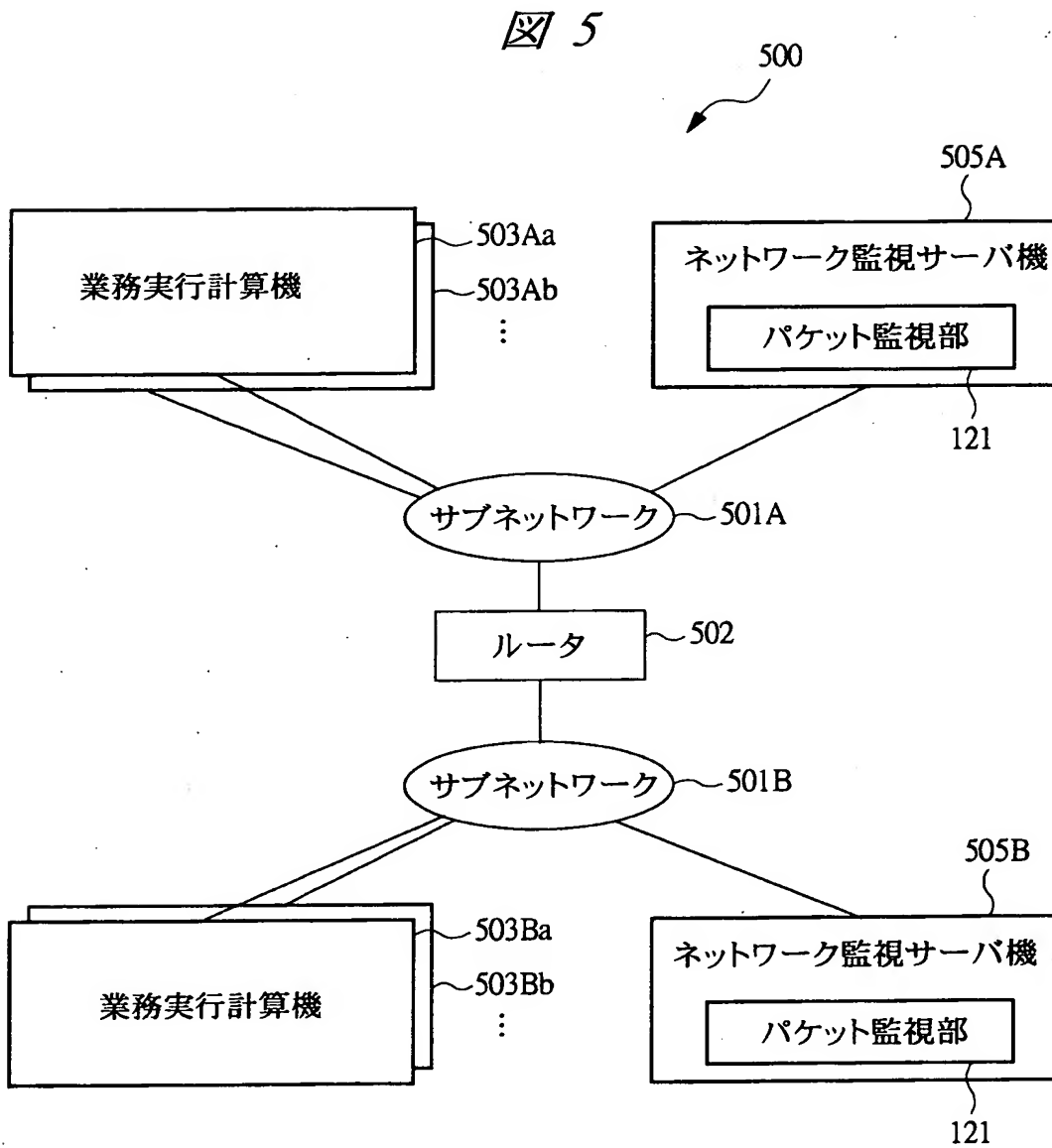


【図 4】

図 4



【図 5】



【書類名】 要約書

【要約】

【課題】 企業のオペレーショナルリスク計量のための内部データを、当該企業内のすべての計算機から収集したか否かを確認できる方法を提供する。

【解決手段】 業務実行計算機 1 0 3 a, 1 0 3 b, …に、その計算機内で発生した損失イベントを収集するためのエージェント 1 1 0 を 1 つ以上設ける。また、その企業のネットワーク 1 0 1 に接続されたネットワーク監視サーバ機 1 0 5 を 1 つ以上設ける。ネットワーク監視サーバ機 1 0 5 は、ネットワーク 1 0 1 を監視し、業務実行計算機 1 0 3 a, 1 0 3 b, …の中に、エージェント 1 1 0 が設けられていない計算機があれば、その旨を監視ログ 1 2 6 に追加することにより、企業内の業務を実行するすべての計算機について、内部データを収集するエージェント 1 1 0 が設けられているか否かを確認できるため、漏れのないオペレーショナルリスク計量が可能となる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所